The Dissertation Committee for Charles Lloyd Samuels
certifies that this is the approved version of the following dissertation:

Auxiliary Polynomials and Height Functions

Committee:

Jeffrey D. Vaaler, Supervisor

John Tate

Fernando Rodriguez-Villegas

Felipe Voloch

Gregory Dresden

Auxiliary Polynomials and Height Functions

by

Charles Lloyd Samuels, B.A.

DISSERTATION

Presented to the Faculty of the Graduate School of

The University of Texas at Austin

in Partial Fulfillment

of the Requirements

for the Degree of

DOCTOR OF PHILOSOPHY

THE UNIVERSITY OF TEXAS AT AUSTIN

August 2007

Acknowledgments

I would like to thank my committee members, Gregory Dresden, Fernando Rodriguez-Villegas, John Tate and Felipe Voloch, for reviewing this dissertation and helping to make it complete. In particular, I thank Fernando Rodriguez-Villegas as well as John Garza for their ideas that inspired me to prove the results that appear here. I also thank Chris Smyth and Michael Mossinghoff for several useful conversations and ideas regarding this work. Finally, I thank my advisor, Jeffrey D. Vaaler, whose teaching and understanding drew my interest in this subject. He provided many hours of discussion and ideas as well as endless emotional support. Always available for conversation, his dedication provided the assistance necessary for me to write a successful dissertation.

Auxiliary Polynomials and Height Functions

Publication No. _____

Charles Lloyd Samuels, Ph.D.
The University of Texas at Austin, 2007

Supervisor: Jeffrey D. Vaaler

We establish two new results in this dissertation. Recent theorems of Dubickas and Mossinghoff use auxiliary polynomials to give lower bounds on the Weil height of an algebraic number α under certain assumptions on α. We prove a theorem which introduces an auxiliary polynomial for giving lower bounds on the height of any algebraic number. In particular, we prove the following theorem.

Theorem. *Let $N \in \mathbb{Z}$ and $\alpha \in \overline{\mathbb{Q}}$. If $T \in \overline{\mathbb{Q}}[x]$ is such that $\deg T \leq N$ and $T(\alpha) \neq 0$ then*

$$U(N, \alpha, T) = U(N, \alpha, 1) = -Nh(\alpha).$$

Our theorem contains, as corollaries, a slight generalization of the above results as well as some new lower bounds in other special cases.

If $\alpha_1, \ldots, \alpha_r$ are algebraic numbers such that

$$N = \sum_{i=1}^{r} \alpha_i \neq \sum_{i=1}^{r} \alpha_i^{-1}$$

for some integer N, then a theorem of Beukers and Zagier [2] gives the best possible lower bound on $\sum_{i=1}^{r} h(\alpha_i)$ where h denotes the logarithmic Weil height. We will extend this result to allow N to be any totally real algebraic number. That is, we establish the following theorem.

Theorem. *Suppose $\alpha_1, \ldots, \alpha_r$ are non-zero algebraic numbers and N is a totally real algebraic integer. If $\alpha_1 + \cdots + \alpha_r = N$ and $\alpha_1^{-1} + \cdots + \alpha_r^{-1} \neq N$ then*

$$\sum_{i=1}^{r} h(\alpha_i) \geq \frac{1}{2} \log \frac{1+\sqrt{5}}{2}$$

with equality when $r = 1$ and $\alpha_1 = \frac{1+\sqrt{5}}{2}$.

This result includes a result of Schinzel [14] which gives a lower bound on the height of a totally real algebraic integer.

Table of Contents

Chapter 1

Introduction

1.1 Absolute Values

An *absolute value* on a field K is a map $|\cdot| : K \to [0, \infty)$ that satisfies the following three conditions:

(i) $|x| = 0$ if and only if $x = 0$

(ii) $|x \cdot y| = |x| \cdot |y|$ for $x, y \in K$

(iii) $|x + y| \leq |x| + |y|$ for $x, y \in K$.

Condition (iii) is known as the *triangle inequality*. If, in addition, $|\cdot|$ satisfies the inequality

$$|x + y| \leq \max\{|x|_p, |y|_p\} \quad \text{for } x, y \in K. \tag{1.1.1}$$

then we say that $|\cdot|$ is *non-archimedean*. Otherwise, we say that it is *archimedean*. Inequality (1.1.1) is called the *strong triangle inequality*. We note that if $|\cdot|$ is non-archimedean and $|x| \neq |y|$ then we have equality in the strong triangle inequality. To see this, assume without loss of generality that $|x| > |y|$ so $|x| \geq |x + y|$. If $|x| > |x + y|$ then

$$|x| = |x + y - y| \leq \max\{|x + y|, |y|\} < |x|$$

which is a contradiction. So we must have that $|x| = |x + y|$.

Every field K has at least one absolute value $|\cdot|_0$ given by

$$|x|_0 = \begin{cases} 1 & \text{if } x \neq 0 \\ 0 & \text{if } x = 0. \end{cases} \tag{1.1.2}$$

This is known as the *trivial* absolute value. All other absolute values on K are called *non-trivial*. We say that two absolute values $|\cdot|_1$ and $|\cdot|_2$ on K are *equivalent* if there exists a positive real number θ such that $|x|_1 = |x|_2^\theta$ for all $x \in K$. It can be shown that this defines an equivalence relation on the set of absolute values on K. An equivalence class of non-trivial absolute values is called a *place* of K. Of course, the trivial absolute value is the unique absolute value in its equivalence class. However, any non-trivial absolute value has many distinct but equivalent absolute values.

Suppose that L is a finite extension of K. Any two equivalent absolute values on L restrict to two equivalent absolute values on K. Hence, each place w of L restricts to a unique place v of K. In this situation we say that w *divides* v and write $w \mid v$. For an absolute value $|\cdot|$ on K define the map $\|\cdot\| : L \to [0, \infty)$ by

$$\|x\| = |\mathrm{Norm}_{L/K}(x)|^{1/[L:K]}. \tag{1.1.3}$$

If $x \in K$ then $\|x\| = |x|$ so that $x \mapsto \|x\|$ extends the absolute value $|\cdot|$ on K to a map on L.

Suppose that X is a vector space of dimension N over K. A *norm* on X with respect to $|\cdot|$ is a map $\|\cdot\| : X \to [0, \infty)$ such that for all $\boldsymbol{x}, \boldsymbol{y} \in X$ and $c \in K$ we have that

(i) $\|\boldsymbol{x}\| = 0$ if and only if $\boldsymbol{x} = \mathbf{0}$

(ii) $\|c\boldsymbol{x}\| = |c| \cdot \|\boldsymbol{x}\|$

(iii) $\|\boldsymbol{x} + \boldsymbol{y}\| \leq \|\boldsymbol{x}\| + \|\boldsymbol{y}\|$

As with absolute values, condition (iii) is called the *triangle inequality*. If $\|\cdot\|$ satisfies the *strong triangle inequality*

$$\|\boldsymbol{x} + \boldsymbol{y}\| \leq \max\{\|\boldsymbol{x}\|_p, \|\boldsymbol{y}\|_p\} \tag{1.1.4}$$

then we say that $\|\cdot\|$ is *non-archimedean*. Conversely, if $\|\cdot\|$ does not satisfy (1.1.4) then we say that $\|\cdot\|$ is *archimedean*.

1.2 Completions

The map $(x, y) \mapsto |x - y|$ defines a metric on K so that $|\cdot|$ induces a metric topology. We say that K is *complete* if it is complete with respect to the metric topology induced by $|\cdot|$. That is, K is complete if every Cauchy sequence in K converges to a point in K. We note that any two equivalent absolute values induce the same metric topology on K. Hence, if $|\cdot|_1$ and $|\cdot|_2$ are equivalent absolute values on K then K is complete with respect to $|\cdot|_1$ if and only if it is complete with respect to $|\cdot|_2$. If K is not complete at v then we may adjoin the limits of all Cauchy sequences in K to obtain a complete field K_v. In view of our remarks above, K_v does not depend on any particular absolute value in v. The field K_v is called the *completion of K at v*.

We now state two important theorems regarding extensions of absolute values in complete fields. The proofs are highly involved so we omit them here.

Theorem 1.2.1. *Let K be a field complete with respect to a non-trivial absolute value $|\cdot|$. If L is a finite extension of K then* (1.1.3) *defines an absolute value $\|\cdot\|$ on L that extends $|\cdot|$. Moreover, $\|\cdot\|$ is the unique extension of $|\cdot|$ to L and L is complete with respect to $\|\cdot\|$.*

We say that a field K is *algebraically closed* if every polynomial with coefficients in K also has its roots in K. We usually write $\overline{K}$ to denote an algebraic closure of K.

Theorem 1.2.2. *Let K be a field complete with respect to the non-trivial absolute value $|\cdot|$. If $\overline{K}$ is an algebraic closure of K then* (1.1.3) *defines an absolute value $\|\cdot\|$ on $\overline{K}$ that extends $|\cdot|$. Moreover, $\|\cdot\|$ is the unique extension of $|\cdot|$ to $\overline{K}$.*

It is worth noting that $\overline{K}$ is not necessarily complete with respect to $\|\cdot\|$.

1.3 Absolute Values on Number Fields

We begin by giving two examples of non-trivial absolute values on $\mathbb{Q}$. First, it is easy to verify that the map $|\cdot|_\infty$ given by

$$|x|_\infty = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0 \end{cases} \tag{1.3.1}$$

is an absolute value on $\mathbb{Q}$. This is known as the *usual absolute value* on $\mathbb{Q}$.

Next, let p be a prime number. For $x \in \mathbb{Q}^\times$ we may write $x = p^a x'$ where $a \in \mathbb{Z}$ and x' is a rational number having no factors of p in its numerator or denominator. We define the *p-adic absolute value* $|\cdot|_p$ by

$$|x|_p = \begin{cases} p^{-a} & \text{if } x \neq 0 \\ 0 & \text{if } x = 0 \end{cases} \tag{1.3.2}$$

It is trivial to see that $|\cdot|_p$ satisfies properties (i) and (ii) in the definition of absolute value so we will simply verify (iii).

First assume that $x, y \in \mathbb{Z}$ and write $x = p^a x'$ and $y = p^b y'$ where p does not divide either x' or y'. Hence, $|x|_p = p^{-a}$ and $|y|_p = p^{-b}$. Of course, we may assume without loss of generality that $|x|_p \geq |y|_p$, and therefore, $a \leq b$. So we find that

$$\begin{aligned} |x+y|_p &= |p^a x' + p^b y'|_p \\ &= |p^a|_p \cdot |x' + p^{b-a} y'|_p. \end{aligned}$$

Since $x' + p^{b-a} y' \in \mathbb{Z}$ we know that $x' + p^{b-a} y'|_p \leq 1$ and we deduce that

$$|x+y|_p \leq |p^a|_p = |x|_p = \max\{|x|_p, |y|_p\} \leq |x|_p + |y|_p \tag{1.3.3}$$

So the triangle inequality holds when x and y are integers. If $x = r_1/s_1$ and

$y = r_2/s_2$ are rational numbers then we have that

$$\begin{aligned}
|x+y|_p &= \left|\frac{r_1}{s_1} + \frac{r_2}{s_2}\right|_p \\
&= \left|\frac{r_1 s_2 + r_2 s_1}{s_1 s_2}\right|_p \\
&\leq \left|\frac{1}{s_1 s_2}\right|_p \max\{|r_1 s_2|_p, |r_2 s_1|_p\} \\
&= \max\{|x|_p, |y|_p\} \\
&\leq |x|_p + |y|_p
\end{aligned}$$

Note that we have in fact established the strong triangle inequality for the p-adic absolute values.

The following theorem due to Ostrowski shows that the usual and p-adic absolute values are all of the non-trivial absolute values on $\mathbb{Q}$, up to equivalence.

Theorem 1.3.1. *Suppose that $|\cdot|$ is a non-trivial absolute value on $\mathbb{Q}$. If $|\cdot|$ is archimedean then it is equivalent to the usual absolute value. If $|\cdot|$ is non-archimedean then it is equivalent to a p-adic absolute value for some prime p.*

In view of Theorem 1.3.1 all non-trivial absolute values on $\mathbb{Q}$ are equivalent to either the usual absolute value or one of the p-adic absolute values. Therefore, we may index the places of $\mathbb{Q}$ by the set $\{\infty, 2, 3, 5, 7, \ldots\}$. So, if K is any number field then each place v of K divides a place p of $\mathbb{Q}$ where p is prime or ∞.

Chapter 2

Height Functions

2.1 Normalized Absolute Values

Let K be a number field of degree d over $\mathbb{Q}$ and let v be a place of K. Then there exists a place p of $\mathbb{Q}$ such that $v \mid p$. We write K_v to denote the completion of K at v and $\mathbb{Q}_p$ to denote the completion of $\mathbb{Q}$ at p. We note that K_v is a finite extension of $\mathbb{Q}_p$ and write $d_v = [K_v : \mathbb{Q}_p]$. We also note the identities

$$d = \sum_{v|p} d_v \tag{2.1.1}$$

and, if $\alpha \in K$,

$$\mathrm{Norm}_{K/\mathbb{Q}}(\alpha) = \prod_{v|p} \mathrm{Norm}_{K_v/\mathbb{Q}_p}(\alpha) \tag{2.1.2}$$

where the sum and product are taken over all places v of K such that $v \mid p$. In particular, (2.1.1) implies that there are at most d places v dividing p.

Next we select two absolute values from the place v. Let $\|\cdot\|_v$ be the unique absolute value on K_v that extends the p-adic absolute value on $\mathbb{Q}_p$. If $p = \infty$ then this extends the usual absolute value on $\mathbb{Q}$. Then let $|\cdot|_v$ be defined by $|x|_v = \|x\|_v^{d_v/d}$ for all $x \in K_v$. Although these absolute values are equal when $K = \mathbb{Q}$, they are equivalent but possibly distinct on an arbitrary number field. The absolute values $\|\cdot\|_v$ are usually more convenient for making

estimates because the triangle equality is sharper when v is archimedean. The absolute values $|\cdot|_v$ are important because they are used in the product formula and to define height functions on $\overline{\mathbb{Q}}$.

If v is non-archimedean, we know only that $K_v/\mathbb{Q}_p$ is a finite extenstion of degree d_v. However, if v is archimedean then we know that d_v equals either 1 or 2. If $d_v = 1$ then the pair $(K_v, \|\cdot\|_v)$ is isometrically isomorphic to $(\mathbb{R}, \|\cdot\|_\infty)$. If $d_v = 2$ then $(K_v, \|\cdot\|_v)$ is isometrically isomorphic to $(\mathbb{C}, \|\cdot\|_\infty)$. For any place v we know that $\|\cdot\|_v$ has a unique extension from the local field K_v to an algebraic closure $\overline{K}_v$. Then it has a further unique extension to a completion Ω_v of $\overline{K}_v$. Of course, the same remarks apply to $|\cdot|_v$. We note that $\Omega_v = \Omega_p$ as a field, but $|\cdot|_v$ and $|\cdot|_p$ are, in general, distinct but equivalent absolute values.

If p is a place of $\mathbb{Q}$ then at each place v of K dividing p we have that

$$\|x\|_v = \|\mathrm{Norm}_{K_v/\mathbb{Q}_p}(x)\|_p^{1/d_v} \quad \text{for } x \in K_v \tag{2.1.3}$$

and therefore

$$|x|_v = |\mathrm{Norm}_{K_v/\mathbb{Q}_p}(x)|_p^{1/d} \quad \text{for } x \in K_v. \tag{2.1.4}$$

If $\alpha \in K$ then $\alpha \in K_v$ for all places v of K so that (2.1.2) implies that

$$\prod_{v|p} |\alpha|_v = |\mathrm{Norm}_{K/\mathbb{Q}}(\alpha)|_p^{1/d} \quad \text{for } \alpha \in K. \tag{2.1.5}$$

By unique factorization of integers we know that if $r \in \mathbb{Q}^\times$ then $|r|_p = 1$ for almost all places p of $\mathbb{Q}$. There are only finitely many places of K dividing

each place of $\mathbb{Q}$ and it can be shown that $|\alpha|_v = 1$ for almost all places v of K. We now establish a fundamental identity known as the *product formula*.

Lemma 2.1.1. *If $\alpha \in K^\times$ then*

$$\prod_v |\alpha|_v = 1. \tag{2.1.6}$$

Proof. In view of our earlier remark, almost all factors in (2.1.6) equal 1, so the left hand side converges. Furthermore, unique factorization of integers implies that that it holds in $\mathbb{Q}$. Hence, we obtain that

$$\begin{aligned}\prod_v |\alpha|_v &= \prod_p \left(\prod_{v|p} |\alpha|_v \right) \\ &= \left(\prod_p |\mathrm{Norm}_{K/\mathbb{Q}}(\alpha)|_p \right)^{1/d} \\ &= 1.\end{aligned}$$

□

Now let L/K be an extension of number fields. Each place w of L determines a unique place v of K such that $w \mid v$ and L_w/K_v is a finite extension. In this situation, we have an analog of (2.1.1)

$$[L : K] = \sum_{w|v} [L_w : K_v] \tag{2.1.7}$$

and an analog of (2.1.2)

$$\mathrm{Norm}_{L/K}(\alpha) = \prod_{w|v} \mathrm{Norm}_{L_w/K_v}(\alpha) \quad \text{for } \alpha \in L. \tag{2.1.8}$$

Since $\|\cdot\|_w$ is an extension of $\|\cdot\|_v$ we obtain that

$$\|x\|_w = \|\mathrm{Norm}_{L_w/K_v}(x)\|_v^{1/[L_w:K_v]} \quad \text{for } x \in L_w. \tag{2.1.9}$$

Thus we get the identity

$$|x|_w = |\mathrm{Norm}_{L_w/K_v}(x)|_v^{1/[L:K]} \quad \text{for } x \in L_w \tag{2.1.10}$$

which, along with (2.1.8), yields

$$\prod_{w|v} |\alpha|_w = |\mathrm{Norm}_{L/K}(\alpha)|_v^{1/[L:K]} \quad \text{for } \alpha \in L. \tag{2.1.11}$$

If we further assume that $\alpha \in K$ then (2.1.11) becomes

$$\prod_{w|v} |\alpha|_w = |\alpha|_v \quad \text{for } \alpha \in K. \tag{2.1.12}$$

2.2 Weil Height

Let us continue examining the situation where L/K is an extension of algebraic number fields and v is a place of K. We will require a modification of (2.1.12), namely,

$$\prod_{w|v} \max\{1, |\alpha|_w\} = \max\{1, |\alpha|_v\} \quad \text{for } \alpha \in K. \tag{2.2.1}$$

To see this, note that if $|\alpha|_v \leq 1$ then $|\alpha|_w \leq 1$ for all places w of L dividing v, so (2.2.1) is trivial. Otherwise, it follows immediately from (2.1.12). In view of (2.2.1) we deduce that

$$\prod_{w} \max\{1, |\alpha|_w\} = \prod_{v} \max\{1, |\alpha|_v\} \quad \text{for } \alpha \in K, \tag{2.2.2}$$

where the products are taken over all places of L and K respectively. Therefore we define the *multiplicative Weil height* $h^* : \overline{\mathbb{Q}} \to [1, \infty)$ in the following way. For $\alpha \in \overline{\mathbb{Q}}$, let K be a number field containing α and let

$$h^*(\alpha) = \prod_v \max\{1, |\alpha|_v\}. \tag{2.2.3}$$

In view of (2.2.2), the right hand side of (2.2.3) does not depend on K. That is, $h^*(\alpha)$ can be computed using any number field containing α.

The function h^* defined in (2.2.3) is a multiplicative version of the Weil height. It is often useful to consider an additive version given by $h(\alpha) = \log h^*(\alpha)$. Of course, we may write the the additive height as

$$h(\alpha) = \sum_v \log^+ |\alpha|_v. \tag{2.2.4}$$

or

$$h(\alpha) = \frac{1}{2} \sum_v |\log |\alpha|_v|_\infty \,. \tag{2.2.5}$$

It is worth noting that (2.2.5) yields the identity

$$h(\alpha^m) = |m|_\infty h(\alpha) \quad \text{for } m \in \mathbb{Z}. \tag{2.2.6}$$

In particular, we note the special case $h(\alpha^{-1}) = h(\alpha)$.

In addition, we observe that h is invariant under Galois conjugation over $\mathbb{Q}$. That is, if α_1 and α_2 have the same minimal polynomial over $\mathbb{Z}$ then

$$h(\alpha_1) = h(\alpha_2). \tag{2.2.7}$$

The proof of (2.2.7) requires the use of the Galois action on places which we will not discuss here.

When restricted to the rational numbers, the Weil height is a very natural measure of complexity. Suppose that r and s are non-zero relatively prime integers. Using the product formula on $\mathbb{Q}$ we find that

$$\begin{aligned} h^*(r/s) &= \prod_p \max\{1, |r/s|_p\} \\ &\quad \left(\prod_p |s|_p\right)\left(\prod_p \max\{1, |r/s|_p\}\right) \\ &= \prod_p \max\{|r|_p, |s|_p\} \end{aligned}$$

Since $(r, s) = 1$ we know that $\max\{|r|_p, |s|_p\} = 1$ for all non-archimedean places p. It follows that

$$h^*(r/s) = \max\{|r|_\infty, |s|_\infty\}. \tag{2.2.8}$$

This observation indicates that the Weil height is indeed a reasonable measurement of complexity on the set of algebraic numbers.

2.3 Projective Height

Let K be a number field of degree d over $\mathbb{Q}$. At each place v of K we write K_v for the completion of K at v and $d_v = [K_v : \mathbb{Q}_p]$, where $v \mid p$. Recall that Ω_v is a complete algebraically closed field containing K_v for each place v. Suppose that N is a non-negative integer and write $\boldsymbol{x} = (x_0, \ldots, x_N)$ to denote a vector in Ω_v^{N+1}. Moreover, define the norms $\|\cdot\|_v$ and $|\cdot|_v$ on Ω_v^{N+1} by

$$\|\boldsymbol{x}\|_v = \max\{\|x_n\|_v : 0 \leq n \leq N\} \tag{2.3.1}$$

and $|\boldsymbol{x}|_v = \|\boldsymbol{x}\|_v^{d_v/d}$ for all $\boldsymbol{x} \in \Omega_v^{N+1}$. We have used the same notation for norms as absolute values, but this causes no ambiguity because norms are applied to vectors and absolute values are applied to scalars. We also note that, in some applications of these norms, it may be valuable to use the Euclidean norm at the non-archimedean places rather than the maximum norm as defined above. In our situation, however, we will find it more relevant to use the maximum norm at all places.

Suppose that L is a finite extension of K. Then, analogous to (2.2.1), we have that

$$\prod_{w|v} |\boldsymbol{\alpha}|_w = |\boldsymbol{\alpha}|_v \quad \text{for } \boldsymbol{\alpha} \in K^{N+1}. \tag{2.3.2}$$

and therefore

$$\prod_{w} |\boldsymbol{\alpha}|_w = \prod_{v} |\boldsymbol{\alpha}|_v \quad \text{for } \boldsymbol{\alpha} \in K^{N+1}. \tag{2.3.3}$$

Hence we may define the *multiplicative projective height* $H^* : \overline{\mathbb{Q}}^{N+1} \setminus \{\mathbf{0}\} \to (0, \infty)$ by

$$H^*(\boldsymbol{\alpha}) = \prod_{v} |\boldsymbol{\alpha}|_v \tag{2.3.4}$$

where the product v runs over places of number field containing all coordinates of $\boldsymbol{\alpha}$. By (2.3.3) this is indeed a function on $\overline{\mathbb{Q}}^{N+1} \setminus \{\mathbf{0}\}$.

If $c \in \overline{\mathbb{Q}}^{\times}$ and $\alpha \in \overline{\mathbb{Q}}^{N+1} \setminus \{\mathbf{0}\}$ then the product formula implies that

$$H^*(c\boldsymbol{\alpha}) = \prod_{v} |c\boldsymbol{\alpha}|_v = \left(\prod_{v} |c|_v \right) \left(\prod_{v} |\boldsymbol{\alpha}|_v \right) = H^*(\boldsymbol{\alpha}). \tag{2.3.5}$$

where the products above run over places v of a number field containing c and the coordinates of $\boldsymbol{\alpha}$. Hence, H^* is well defined on N-dimensional projective

space $\mathbb{P}^N(\overline{\mathbb{Q}})$. Since we may select a representative of each vector in $\mathbb{P}^N(\overline{\mathbb{Q}})$ that has at least one homogeneous coordinate equal to 1, we also find that $H^* : \mathbb{P}^N(\overline{\mathbb{Q}}) \to [1, \infty)$. As before we write $H(\boldsymbol{\alpha}) = \log H^*(\boldsymbol{\alpha})$ for the additive version of the projective height and note that

$$H(\boldsymbol{\alpha}) = \sum_v \log |\boldsymbol{\alpha}|_v = \sum_v \log \max\{|\alpha_0|_v, \ldots, |\alpha_N|_v\} \tag{2.3.6}$$

It is worth noting that if $\alpha \in \overline{\mathbb{Q}}^\times$ then

$$H((1 : \alpha)) = h(\alpha) \tag{2.3.7}$$

so that we may think of the projective height as a generalization of the Weil height.

2.4 Global Supremum Norm

Let K be a number field and v a place of K. Again, Ω_v is a complete algebraically closed field containing K_v and we write $\boldsymbol{x} = (x_0, \ldots, x_N)$ for a generic element of Ω_v^{N+1}. Define the local supremum norm on the unit ball to be the map $\nu_v^* : \Omega_v[\boldsymbol{x}] \to [0, \infty)$ given by

$$\nu_v^*(T) = \sup\{|T(\boldsymbol{x})|_v : \boldsymbol{x} \in \Omega_v^{N+1},\ |\boldsymbol{x}|_v \leq 1\} \tag{2.4.1}$$

where $|\cdot|_v$ is the norm given in the previous section. It is trivial to verify that ν_v^* does indeed define a norm on the $(N+1)$-dimensional vector space Ω_v^{N+1}.

Moreover, ν_v^* is easily computed when v is non-archimedean. If T has coefficient vector $(a_0, \ldots, a_M)$ then

$$\nu_v^*(T) = \max\{|a_0|_v, \ldots, |a_M|_v\} \quad \text{for } v \nmid \infty. \tag{2.4.2}$$

When v is archimedean the situation is not as simple, although the triangle inequality implies that

$$\nu_v^*(T) \leq \left(\sum_{m=0}^{M} \|a_m\|_v \right)^{d_v/d} \quad \text{for } v \mid \infty. \tag{2.4.3}$$

We define the additive version of the local supremum norm $\nu_v(T) = \log \nu_v^*(T)$.

If we further assume that T has coefficients in K then we may define the *multiplicative global supremum norm* $\nu^* : K[\boldsymbol{x}] \to [0, \infty)$ by

$$\nu^*(T) = \prod_v \nu_v^*(T) \tag{2.4.4}$$

where v runs over all places of K. As before, this definition does not depend on K so we have in fact defined a function $\nu^* : \overline{\mathbb{Q}}[\boldsymbol{x}] \to [0, \infty)$. Furthermore, for $T \neq 0$ we will often use the additive version of the global supremum norm

$$\nu(T) = \log \nu^*(T) = \sum_v \log \nu_v^*(T) \tag{2.4.5}$$

Chapter 3

Lehmer's Problem

3.1 Mahler Measure and Lehmer's Problem

Let f be a polynomial with complex coefficients given by

$$f(z) = a\prod_{n=1}^{N}(z-\alpha_n).$$

For this chapter, let $|\cdot|$ denote the usual absolute value on $\mathbb{C}$. We define the *logarithmic Mahler measure* of f by

$$\mu(f) = \int_0^1 \log|f(e^{2\pi it})|dt \tag{3.1.1}$$

and it follows from Jensen's formula that

$$\mu(f) = \log|a| + \sum_{n=1}^{N}\log^+|\alpha_n|. \tag{3.1.2}$$

If $g \in \mathbb{C}[z]$ then we see easily that

$$\mu(f\cdot g) = \mu(f) + \mu(g). \tag{3.1.3}$$

If we further assume that f has integer coefficients, we see that $\mu(f) \geq 0$. Moreover, Kronecker's Theorem shows that $\mu(f) = 0$ if and only if f is a product of cyclotomic polynomials and $\pm x$. In a famous 1933 paper, D.H.

Lehmer [9] asked if there exists a positive constant c such that $\mu(f) \geq c$ for all $f \in \mathbb{Z}[x]$. He noted that the polynomial

$$\ell(x) = x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1 \tag{3.1.4}$$

satisfies $\mu(f) = 0.1623576\ldots$ and this remains the smallest known positive Mahler measure. We note that in view of (3.1.2) and (3.1.3) it is enough to consider monic irreducible polynomials with integer coefficients when approaching Lehmer's problem.

3.2 Progress on Lehmer's Problem

Since Lehmer's problem in its original form is concerned only with polynomials f having integer coefficients, we will assume for the remainder of this section that $f \in \mathbb{Z}[x]$. The best known universal result toward answering Lehmer's problem is a theorem of Dobrowolski [7] which states that

$$\mu(f) \gg \left(\frac{\log \log \deg f}{\log \deg f} \right)^3. \tag{3.2.1}$$

That is, $\mu(f)$ is bounded from below by a term that tends to zero slowly as $\deg f \to \infty$.

Although Dobrowolski's theorem is the best known universal lower bound on the Mahler measure, an affirmative answer to Lehmer's problem has been given in certain special cases. Schinzel [14] showed that if all roots of f are real algebraic integers then

$$\mu(f) \geq \deg f \cdot \frac{\mu(x^2 - x - 1)}{2} = \deg f \cdot \frac{1 + \sqrt{5}}{4}. \tag{3.2.2}$$

We attain equality in this inequality by taking $f(x) = x^2 - x - 1$. Moreover, (3.2.2) indicates that $\mu(f)$ tends to ∞ as $\deg f \to \infty$. Hence, polynomials having only real roots satisfy a stronger condition than is predicted by Lehmer's problem. A similiar situation occurs when all roots of f lie in an abelian Galois extension of $\mathbb{Q}$. Amoroso and Dvornicich [1] showed that if f is such a polynomial but not x or cyclotomic then

$$\mu(f) \geq \deg f \cdot \frac{\log 5}{12}. \tag{3.2.3}$$

Unlike Schinzel's result, it remains an open problem to determine the best possible lower bound in this situation.

We say that a polynomial f is reciprocal if whenever α is a root of f then α^{-1} is also a root of f. Breusch [6] showed that there exists $c > 0$ such that if f is not reciprocal then $\mu(f) \geq c$. Later, Smyth [15] showed that we may take $c = \mu(x^3 - x - 1)$, thus giving the best possible lower bound in this case. In other words, he established the inequality

$$\mu(f) \geq \mu(x^3 - x - 1) = 0.2776\ldots \tag{3.2.4}$$

for f not reciprocal. We note that the polynomial $\ell(x)$ as in (3.1.4) is reciprocal so that Smyth's theorem does not apply.

Recently, Borwein, Hare and Mossinghoff [5] were able to improve Smyth's bound in the special case that f has odd coefficients. In this situation, they showed that

$$\mu(f) \geq \mu(x^2 - x - 1) = \log \frac{1 + \sqrt{5}}{2}. \tag{3.2.5}$$

Borwein, Dobrowolski and Mossinghoff [4] relaxed the assumption that f not be reciprocal and still obtained an absolute lower bound on $\mu(f)$. They used properties of the resultant to prove that if f has no cyclotomic factors and coefficients congruent to $1 \mod m$ then

$$\mu(f) \geq c_m \cdot \frac{\deg f}{1 + \deg f}$$

where $c_2 = (\log 5)/4$ and $c_m = \log(\sqrt{m^2+1}/2)$ for all $m > 2$. These results appear in [4] as Corollaries 3.4 and 3.5 to Theorem 3.3. This theorem gives a lower bound of the form

$$\mu(f) \geq c_m(T) \cdot \frac{\deg f}{1 + \deg f} \tag{3.2.6}$$

where f has no cyclotomic factors and coefficients congruent to $1 \mod m$. Here, $c_m(T)$ is a positive constant depending on both m and an auxiliary polynomial $T \in \mathbb{Z}[x]$. The corollaries follow by making an appropriate choice of T.

Extending the techniques of [4], Dubickas and Mossinghoff [8] improved inequality (3.2.6) by finding a lower bound of the form

$$\mu(g) \geq b_m(T) \cdot \frac{\deg g}{1 + \deg f} \tag{3.2.7}$$

where $b_m(T) \geq c_m(T)$. Here, g has no cyclotomic factors and is a factor of a polynomial f having coefficients congruent to $1 \mod m$. Moreover, they produced an algorithm which generates a sequence of polynomials $\{T_k\}$ such that the sequence $\{b_m(T_k)\}$ is increasing and $b_m(T_k) > c_m$ for sufficiently large k.

3.3 Weil Height in Lehmer's Problem

If $f \in \mathbb{Z}[x]$ has relatively prime coefficients, then $\mu(f)$ is related to the heights of the roots of f by the indentity

$$\mu(f) = \sum_{n=1}^{N} h(\alpha_n). \tag{3.3.1}$$

If, in addition, f is irreducible then (2.2.7) implies that

$$\mu(f) = [\mathbb{Q}(\alpha) : \mathbb{Q}] \cdot h(\alpha) \tag{3.3.2}$$

where α is any root of f. This means that Lehmer's problem may be reformulated in the following way. Does there exist a positive constant c such that

$$\deg \alpha \cdot h(\alpha) \geq c \tag{3.3.3}$$

for all algebraic numbers α different from 0 and the roots of unity? In view of this reformulation of Lehmer's problem, it is valuable to give lower bounds on the Weil height in special cases.

In view of (3.3.2), the result of Amoroso and Dvornicich in (3.2.3) may be expressed as

$$h(\alpha) \geq \frac{\log 5}{12} \tag{3.3.4}$$

for all algebraic numbers α that lie in an abelian extenstion of $\mathbb{Q}$. Furthermore, the result of Schinzel given in (3.2.2) may be restated as

$$h(\alpha) \geq \frac{1}{2} \log \frac{1+\sqrt{5}}{2} \tag{3.3.5}$$

for all totally real algebraic integers α. Bombieri and Zannier [3] proved that if α is a totally p-adic algebraic number, not 0 or a root of unity then $h(\alpha) \geq \frac{\log p}{2(p+1)}$.

If, in addition, α is an algebraic unit, Petsche [11] gave the improved lower bound

$$h(\alpha) \geq \frac{c_p}{p-1} \tag{3.3.6}$$

where $c_2 = \log(\sqrt{2})$ and $c_p = \log(p/2)$ for all primes $p > 2$. Dubickas and Mossinghoff [8] introduced an auxiliary polynomial in this problem as well, giving the lower bound

$$h(\alpha) \geq \frac{b_p(T)}{p-1} \tag{3.3.7}$$

where $b_p(T)$ is the same as in (3.2.7). They showed how to find a sequence of auxiliary polynomials that further improved (3.3.6).

As we have remarked, the well-known lower bounds (3.2.6), (3.2.7) and (3.3.7) all rely on an auxiliary polynomial T. However, each of these bounds requires an assumption on α. The author [13] showed that if α is any algebraic number then $h(\alpha)$ can be expressed in terms of an auxiliary polynomial. Furthermore, this function naturally recovers the results of [8] as well as two other interesting conesequences. These results are given in chapter 4.

Zhang [17] established slightly different but related result. As a consequence of a more general theorem, he showed that there exists $c > 0$ such

that

$$h(\alpha) + h(1-\alpha) \geq c \tag{3.3.8}$$

whenever α is not 0, 1 or a primitive 6th root of unity. Zagier [16] used elementary methods to show that (3.3.8) holds with $c = \frac{1}{2}\log\frac{1+\sqrt{5}}{2}$ with cases of equality identified. As Zagier notes, it is interesting that this is the same lower bound that appears in Schinzel's bound (3.3.5) on the height of a totally real algebraic integer.

Beukers and Zagier [2] generalized the results of [16] in the following way. Let $\alpha_1, \ldots, \alpha_r$ be non-zero algebraic numbers such that $\alpha_1 + \cdots + \alpha_r = N$ and $\alpha_1^{-1} + \cdots + \alpha_r^{-1} \neq N$ for some integer N. Then

$$\sum_{i=1}^{r} \log h(\alpha_i) \geq \frac{1}{2}\log\frac{1+\sqrt{5}}{2} \tag{3.3.9}$$

with cases of equality. This result follows from a more general theorem concerning the projective heights of algebraic points. The author [12] generalized the methods of [2] to show that (3.3.9) holds even if we take N to be a totally real algebraic integer. Although this generalization is only slight, it is interesting because it contains Schinzel's bound (3.3.5) by taking $r = 1$. We present this result in chapter 5.

Chapter 4

The Weil Height in Terms of an Auxiliary Polynomial [13]

4.1 Main Results

Recall that Ω_v is the completion of an algebraic closure of K_v. For $\alpha \in \Omega_v$ and $N \in \mathbb{Z}$ such that $\deg T \leq N$ define

$$U_v(N, \alpha, T) = \inf\{\nu_v(T - f) : f \in \Omega_v[x], f(\alpha) = 0 \text{ and } \deg f \leq N\}$$

where ν_v denotes the logarithm of the local supremum norm on Ω_v. We now obtain the following lemma which relates $U_v(N, \alpha, T)$ to more familiar functions.

Lemma 4.1.1. *Let $N \in \mathbb{Z}$ and $\alpha \in \Omega_v$. If $T \in \Omega_v[x]$ is such that $\deg T \leq N$ then*

$$\begin{aligned} U_v(N, \alpha, T) &= \log |T(\alpha)|_v + U_v(N, \alpha, 1) \\ &= \log |T(\alpha)|_v - N \log^+ |\alpha|_v. \end{aligned} \tag{4.1.1}$$

Proof. If $T(\alpha) = 0$ then all parts of equations (4.1.1) equal $-\infty$, so we assume that $T(\alpha) \neq 0$. Let us first verify the left hand equation. For simplicity define the set

$$S_v(\alpha, N) = \{f \in \Omega_v[x] : f(\alpha) = 0 \text{ and } \deg f \leq N\}.$$

It is clear that

$$\begin{aligned} U_v(N,\alpha,T) &= \inf\{\nu_v(T(x)-f(x)) : f \in S_v(\alpha,N)\} \\ &= \inf\{\nu_v(T(x)-(T(x)-T(\alpha)+f(x))) : f \in S_v(\alpha,N)\} \\ &= \inf\{\nu_v(T(\alpha)-f(x)) : f \in S_v(\alpha,N)\} \\ &= \inf\{\nu_v(T(\alpha)(1-f(x))) : f \in S_v(\alpha,N)\}. \end{aligned}$$

Since ν_v is the logarithm of a norm, we may factor $T(\alpha)$ out of the infimum to see that

$$\begin{aligned} U_v(N,\alpha,T) &= \log|T(\alpha)|_v + \inf\{\nu_v(1-f(x)) : f \in S_v(\alpha,N)\} \\ &= \log|T(\alpha)|_v + U_v(N,\alpha,1) \end{aligned}$$

which establishes the first equality.

In order to establish the second equality we must show that $U_v(N,\alpha,1) = -N\log^+|\alpha|_v$. We first claim that if $N \in \mathbb{Z}$ then

$$\log|F(\alpha)|_v \le \nu_v(F) + N\log^+|\alpha|_v \tag{4.1.2}$$

for all $F \in \Omega_v[x]$ with $\deg F \le N$. To see this, write $F(x) = \sum_{k=0}^{\deg F} a_k x^k$. If v is non-Archimedean then (4.1.2) follows from (2.4.2) and the strong triangle inequality. We now assume that v is Archimedean. If $|\alpha|_v \le 1$ then the inequality follows from the maximum principle. If $|\alpha|_v > 1$ then we obtain that

$$\log|\alpha^{-\deg F}F(\alpha)|_v \le \nu_v(x^{\deg F}F(x^{-1})) = \nu_v(F)$$

and (4.1.2) follows.

Now suppose that $f \in S_v(\alpha, N)$. Therefore, $\deg(1-f) \leq N$ and inequality (4.1.2) implies that

$$0 = \log|1 - f(\alpha)|_v \leq \nu_v(1-f) + N\log^+|\alpha|_v.$$

This inequality holds for all polynomials $f \in S_v(\alpha, N)$ so that the right hand side may be replaced by its infimum over all such f. That is, we obtain $0 \leq U_v(N, \alpha, 1) + N\log^+|\alpha|_v$ so we find that

$$U_v(N, \alpha, 1) \geq -N\log^+|\alpha|_v. \tag{4.1.3}$$

We will now establish the opposite direction of (4.1.3) by making specific choices for f to give upper bounds on $U_v(N, \alpha, 1)$. By taking $f \equiv 0$ we see easily that $U_v(N, \alpha, 1) \leq 0$. Similarly, by taking $f(x) = 1 - (x/\alpha)^N$ we obtain

$$U_v(N, \alpha, 1) \leq \nu_v(x/\alpha)^N = -N\log|\alpha|_v.$$

Hence

$$U_v(N, \alpha, 1) \leq \min\{0, -N\log|\alpha|_v\} = -N\log^+|\alpha|_v. \tag{4.1.4}$$

□

If $\alpha \in K$ and $T \in K[x]$ are such that $T(\alpha) \neq 0$ then Lemma 4.1.1 implies that $U_v(N, \alpha, T) = 0$ for all but finitely many places v of K. Hence, in this situation we may define

$$U(N, \alpha, T) = \sum_v U_v(N, \alpha, T)$$

where v runs over the places of K. We note that this definition does not depend on K so that U is a well-defined function on $\{(\alpha, T) \in \overline{\mathbb{Q}} \times \overline{\mathbb{Q}}[x] : T(\alpha) \neq 0\}$. We are now prepared to state and prove our main result.

Theorem 4.1.2. *Let $N \in \mathbb{Z}$ and $\alpha \in \overline{\mathbb{Q}}$. If $T \in \overline{\mathbb{Q}}[x]$ is such that $\deg T \leq N$ and $T(\alpha) \neq 0$ then*

$$U(N, \alpha, T) = U(N, \alpha, 1) = -Nh(\alpha).$$

Proof. Assume that K is a number field containing α and the coefficients of T and v is a place of K. We know that the absolute value $|\cdot|_v$ satisfies the product formula $\prod_v |\beta|_v = 1$ for all $\beta \in K^\times$. Hence, summing the equation of Lemma 4.1.1 over all places v of K we get that

$$U(N, \alpha, T) = U(N, \alpha, 1) = -Nh(\alpha) \tag{4.1.5}$$

which establishes the theorem. □

4.2 Polynomials near $x^n - 1$

As we have remarked, Theorem 4.1.2 naturally generalizes the results of Dubickas and Mossinghoff in [8]. We will give a single result that contains both their bound on the Mahler measure of a polynomial having coefficients congruent to 1 mod m and their bound on the height of a totally p-adic algebraic unit.

Let us begin by reconstructing the situation of [8]. For an auxiliary

polynomial $T \in \mathbb{Z}[x]$ and a positive integer m define

$$\omega_m(T) = \log \gcd \left\{ \frac{m^k T^{(k)}(1)}{k!} : 0 \leq k \leq \deg T \right\}. \tag{4.2.1}$$

Also assume that f is a polynomial of degree $n-1$ with integer coefficients congruent to 1 mod m. The authors prove (Theorem 2.2 of [8]) that if g is a factor of f over $\mathbb{Z}$ satisfying $\gcd(g(x), T(x^n)) = 1$ then

$$\mu(g) \geq \frac{\omega_m(T) - \nu_\infty(T)}{\deg T} \left(\frac{\deg g}{n} \right). \tag{4.2.2}$$

Later they prove (Theorem 4.2 of [8]) that if α is a totally p-adic algebraic unit then

$$h(\alpha) \geq \frac{\omega_p(T) - \nu_\infty(T)}{(p-1)\deg T}. \tag{4.2.3}$$

Our goal is to produce a generalization of (4.2.2) where T and f are allowed to have algebraic coefficients. Our version also contains (4.2.3) as a corollary.

Before we begin, we make one final trivial remark regarding the hypotheses of [8]. The assumption that f have degree $n-1$ and coefficients congruent to 1 mod m is equivalent to the assumption that $(x-1)f(x) \equiv x^n - 1 \mod m$. Therefore, we can make a slightly stronger conclusion by hypthesizing instead that $f(x) \equiv x^n - 1 \mod m$ and bounding the Mahler measure of all factors g of f.

We will require a version of $\omega_m(T)$ defined in (4.2.1) that allows m to be a general algebraic number and T to have any algebraic coefficients. If K is a number field, $m \in K$ and $T \in K[x]$ define

$$\omega_m(T) = -\sum_{v \nmid \infty} \log \max \left\{ \left| \frac{m^k T^{(k)}(1)}{k!} \right|_v : 0 \leq k \leq \deg T \right\} \tag{4.2.4}$$

where the sum is taken over places v of K. By the way we have normalized our absolute values, this definition does not depend on K. Moreover, if $m \in \mathbb{Z}$ and $T \in \mathbb{Z}[x]$ then (4.2.4) is the same as the definition (4.2.1).

If $\alpha, \beta, m \in K$, then we write $\alpha \equiv \beta \mod m$ if $|\alpha - \beta|_v \leq |m|_v$ for all $v \nmid \infty$. Similarly, if $f, g \in K[x]$ we write $f \equiv g \mod m$ if $\nu_v(f-g) \leq \log |m|_v$ for all $v \nmid \infty$. Neither defintion depends on K and both generalize the usual notions of congruence in $\mathbb{Z}$. If $T \in K[x]$ we often write $\nu_\infty(T) = \sum_{v|\infty} \nu_v(T)$ where v runs over places of K. This notation again does not depend on K. It will also be convenient for this section and future applications to define $U_v(\alpha, T) = U_v(\deg T, \alpha, T)$ and $U(\alpha, T) = U(\deg T, \alpha, T)$.

Using the definitions above, we obtain our generalized version of the results of [8].

Theorem 4.2.1. *Let m be an algebraic number. Suppose that $f \in \overline{\mathbb{Q}}[x]$ has degree n and $f(x) \equiv x^n - 1 \mod m$. If α is a root of f and $T \in \overline{\mathbb{Q}}[x]$ is such that $T(\alpha^n) \neq 0$ then*

$$h(\alpha) \geq \frac{\omega_m(T) - \nu_\infty(T)}{n \deg T}.$$

Proof. Let K be a number field containing α and the coefficients of T and let v index the places of K. Using Theorem 4.1.2 with $N = n \deg T$ and $T(x^n)$ in place of $T(x)$ we see that

$$-n \deg T \cdot h(\alpha) \leq \sum_{v \nmid \infty} U_v(\alpha, T(x^n)) + \nu_\infty(T) \tag{4.2.5}$$

so we must show that $\sum_{v\nmid\infty} U_v(\alpha, T(x^n)) \leq -\omega_m(T)$. Let $v \nmid \infty$. Writing T in its Taylor expansion at 1 and using the binomial theorem we find that

$$\begin{aligned} U_v(\alpha, T(x^n)) &= U_v\left(\alpha, \sum_{k=0}^{\deg T} \frac{T^{(k)}(1)}{k!}(x^n-1)^k\right) \\ &\leq \nu_v\left(\sum_{k=0}^{\deg T} \frac{T^{(k)}(1)}{k!}(x^n-1-f(x))^k\right). \end{aligned}$$

Then using the strong triangle inequality for ν_v we obtain

$$U_v(\alpha, T(x^n)) \leq \max\left\{\log\left|\frac{T^{(k)}(1)}{k!}\right|_v + k\nu_v(x^n-1-f(x)) : 0 \leq k \leq \deg T\right\}.$$

Since $f(x) \equiv x^n - 1 \mod m$ we have that $\nu_v(x^n-1-f(x)) \leq \log|m|_v$. Consequently, we obtain that

$$\sum_{v\nmid\infty} U_v(\alpha, T(x^n)) \leq \sum_{v\nmid\infty} \log\max\left\{\left|\frac{m^k T^{(k)}(1)}{k!}\right|_v : 0 \leq k \leq \deg T\right\} = -\omega_m(T)$$

and the theorem follows from (4.2.5). □

If we assume that f and T have integer coefficients and m is a positive integer then we recover Theorem 2.2 of [8].

Corollary 4.2.2. *Let $f \in \mathbb{Z}[x]$ have degree n and $f(x) \equiv x^n - 1 \mod m$. If g is a factor of f and $T \in \mathbb{Z}[x]$ is such that $\gcd(g(x), T(x^n)) = 1$ then*

$$\mu(g) \geq \frac{\omega_m(T) - \nu_\infty(T)}{\deg T}\left(\frac{\deg g}{n}\right).$$

Proof. Apply Theorem 4.2.1 to each root α of g and the result follows. □

We also recover Theorem 4.2 of [8] giving a lower bound on the height of a totally p-adic algebraic unit.

Corollary 4.2.3. *If α is a totally p-adic algebraic unit and $T \in \mathbb{Z}[x]$ is such that $T(\alpha^{p-1}) \neq 0$ then*

$$h(\alpha) \geq \frac{\omega_p(T) - \nu_\infty(T)}{(p-1)\deg T}.$$

Proof. For a general number field K and a non-Archimedean place v of K dividing the place p of $\mathbb{Q}$, let $O_v = \{x \in K_v : |x|_v \leq 1\}$ denote the ring of v-adic integers in K_v and let π_v be a generator of its unique maximal ideal $M_v = \{x \in K_v : |x|_v < 1\}$. Let $d_v = [K_v : \mathbb{Q}_p]$ denote the local degree and $d = [K : \mathbb{Q}]$ the global degree. We also define the residue degree f_v by $p^{f_v} = |O_v/M_v|$ and note that $|\pi_v|_v = \|p\|_v^{f_v/d}$. If K is a totally p-adic field then we have that $f_v = d_v = 1$ for all $v \mid p$.

Now assume that K is the totally p-adic field $\mathbb{Q}(\alpha)$. If v is a place of K dividing p then

$$|\alpha^{p-1} - 1|_v \leq |\pi_v|_v = \|p\|_v^{f_v/d} = \|p\|_v^{d_v/d} = |p|_v$$

and if v does not divide p or ∞ then

$$|\alpha^{p-1} - 1|_v \leq 1 = |p|_v.$$

Hence we have that $x^{p-1} - 1 \equiv x^{p-1} - \alpha^{p-1} \mod p$. Now we may apply Theorem 4.2.1 with $m = p$ and $f(x) = x^{p-1} - \alpha^{p-1}$ and the result follows. □

4.3 Polynomials near $(x^n - 1)^r$

In this section, we apply Theorem 4.1.2 in order to examine the Mahler measure of any factor of a polynomial f satsifying $f(x) \equiv (x^n - 1)^r \mod m$.

In particular, we obtain the following explicit lower bound.

Theorem 4.3.1. *Suppose that $f \in \mathbb{Z}[x]$ has degree nr, $m \geq 2$ is an integer, and $f(x) \equiv (x^n - 1)^r \mod m$. If g is a factor of f over $\mathbb{Z}$ having no cyclotomic factors then*

$$\mu(g) \geq c \cdot \left(\frac{\deg g}{n 2^r} \right)$$

where c is the unique positive real number satisfying $ce^{c/2} \log 3 = \log(3/2) \log 2$. (Note that $c = .22823\ldots$).

As an application, let T be a product of cyclotomic polynomials of degree $2N$. Then we may apply Theorem 4.3.1 with $g(x) = T(x) + mx^N$ where $|m| \geq 2$. In this situation, r is the maximum multiplicity of the cyclotomic polynomials in the factorization of T over $\mathbb{Z}$. These types of polynomials have been studied extensively (see, for example, [10]) and our results yield a lower bound on any such g, although it is not absolute for this entire class of polynomials.

Of course, Theorem 4.3.1 is not helpful when g is a product of cyclotomic polynomials with the middle coefficient shifted by only 1. Numerical evidence presented in [10] suggests that these polynomials form a relatively rich collection of polynomials of small Mahler measure. Hence it would be useful to have a method for giving lower bound on their Mahler measure. However, we are unable to do so in this dissertation.

We also note that Theorem 4.3.1 is weaker than Corollaries 3.3 and 3.4 of [4] when $r = 1$. In this situation, we may appeal to [8] or the results section

4.2 to obtain the sharpest known bounds.

The proof of Theorem 4.3.1 will require 3 lemmas as well as some additional notation. Suppose that g and T are polynomials over any field K. $K[x]$ is certainly a unique factorization domain so we may write $\lambda_g(T)$ to denote the mulitplicity of g in the factorization of T. If G is a collection of polynomials over K, then let $\lambda_G(T) = \sum_{g \in G} \lambda_g(T)$.

Our first lemma is a direct generalization of Theorem 3.3 of [4].

Lemma 4.3.2. *Suppose that $f \in \mathbb{Z}[x]$ has degree nr and $f(x) \equiv (x^n - 1)^r$ mod m. If g is a factor of f over $\mathbb{Z}$ and $T \in \mathbb{Q}[x]$ is relatively prime to g then*

$$\mu(g) \geq \frac{\lambda_{x^n-1}(T) \log m - r\nu_\infty(T)}{r \deg T} \cdot \deg g. \tag{4.3.1}$$

Moreover, if $2|m$ then

$$\mu(g) \geq \frac{\lambda_{x^n-1}(T) \log m + \lambda_{G_n}(T) \log 2 - r\nu_\infty(T)}{r \deg T} \cdot \deg g \tag{4.3.2}$$

where $G_n = \{x^{n2^j} + 1 : j \geq 0\}$.

Proof. Suppose that α is a root of f, K is a number field containing α and v indexes the places of K. First observe that if $F_1, F_2 \in \Omega_v[x]$ then $\nu_v(F_1F_2) \leq \nu_v(F_1) + \nu_v(F_2)$. This yields the multiplicative inequality

$$U_v(\alpha, F_1F_2) \leq U_v(\alpha, F_1) + U_v(\alpha, F_2). \tag{4.3.3}$$

Theorem 4.1.2 implies that

$$-r \deg T \cdot h(\alpha) \leq \sum_{v \nmid \infty} U_v(\alpha, T^r) + r\nu_\infty(T). \tag{4.3.4}$$

Suppose that that $T_0 \in \mathbb{Z}[x]$ is such that $T(x)^r = (x^n-1)^{r\lambda_{x^n-1}(T)}T_0(x)$. We know that since T_0 has integer coefficients, $U_v(\alpha, T_0) \leq \nu_v(T_0) \leq 0$. Then (4.3.3) implies that

$$\begin{aligned} U_v(\alpha, T^r) &\leq \lambda_{x^n-1}(T)U_v(\alpha, (x^n-1)^r) \\ &\leq \lambda_{x^n-1}(T)\nu_v((x^n-1)^r - f(x)). \end{aligned}$$

Since f has integer coefficients and satisfies $f(x) \equiv (x^n-1)^r \mod m$ we know that $\sum_{v\nmid\infty} \nu_v((x^n-1)^r - f(x)) \leq -\log m$. It follows that

$$-r\deg T \cdot h(\alpha) \leq -\lambda_{x^n-1}(T)\log m + r\nu_\infty(T). \tag{4.3.5}$$

Applying (4.3.5) to each root α of g, we obtain (4.3.1).

Next, assume that $2|m$. In this situation, write

$$T(x)^r = T_0(x)(x^n-1)^{r\lambda_{x^n-1}(T)}\prod_{j\geq 0}(x^{n2^j}+1)^{r\lambda_{x^{n2^j}+1}(T)}$$

for some $T_0 \in \mathbb{Z}[x]$. In addition to the congruence $f(x) \equiv (x^n-1)^r \mod m$, for each $j \geq 0$ there exists $b_j \in \mathbb{Z}[x]$ such that $f(x)b_j(x) \equiv (x^{n2^j}+1)^r \mod 2$. Hence, it follows that

$$\sum_{v\nmid\infty} \nu_v(x^{n2^j}+1-f(x)b_j(x)) \leq -\log 2$$

for all $j \geq 0$. Now we find that

$$U_v(\alpha, T^r) \leq \lambda_{x^n-1}(T)\nu_v((x^n-1)^r - f(x)) + \sum_{j\geq 0}\lambda_{x^{n2^j}+1}(T)\nu_v(x^{n2^j}+1-f(x)b_j(x))$$

for all $v \nmid \infty$. Therefore, (4.3.4) yields

$$-r\deg T \cdot h(\alpha) \leq -\lambda_{x^n-1}(T)\log m - \lambda_{G_n}(T)\log 2 + r\nu_\infty(T)$$

and the result follows by a similar argument as above. □

Note that the right hand sides of the inequalities of Lemma 4.3.2 are less than 0 when r is large compared to m. Hence, it may appear that these bounds are useful only when r is small. However, a simple consequence of Lemma 4.3.2 allows us to give non-trivial lower bounds when r is large.

Lemma 4.3.3. *Let p be prime and q a power of p such that $\deg f = nq$ and $f(x) \equiv (x^n - 1)^q \mod p$. If g is a factor of f over $\mathbb{Z}$ and $T \in \mathbb{Q}[x]$ is such that $\gcd(T(x^q), g(x)) = 1$ then*

$$\mu(g) \geq \frac{\lambda_{x^n-1}(T)\log p - \nu_\infty(T)}{q \deg T} \cdot \deg g. \tag{4.3.6}$$

Moreover, if $p = 2$ then

$$\mu(g) \geq \frac{(\lambda_{x^n-1}(T) + \lambda_{G_n}(T))\log 2 - \nu_\infty(T)}{q \deg T} \cdot \deg g \tag{4.3.7}$$

where $G_n = \{x^{n2^j} + 1 : j \geq 0\}$.

Proof. We know that $f(x) \equiv (x^n - 1)^q \equiv x^{nq} - 1 \mod p$. Therefore, we may apply Lemma 4.3.2 with $m = p$, $r = 1$ and $T(x^q)$ in place of $T(x)$. We obtain that

$$\begin{aligned}\mu(g) &\geq \frac{\lambda_{x^{nq}-1}(T(x^q))\log p - \nu_\infty(T(x^q))}{q \deg T} \cdot \deg g \\ &= \frac{\lambda_{x^n-1}(T)\log p - \nu_\infty(T)}{q \deg T} \cdot \deg g.\end{aligned}$$

Inequality (4.3.7) follows from a similar argument. □

In the hypotheses of Lemma 4.3.2 we are given $f(x) \equiv (x^n - 1)^r \mod m$, so we may also apply Lemma 4.3.3 with p a prime dividing m and $q = p^{\lceil \log_p r \rceil}$. We know that $(x^n-1)^{q-r} f(x) \equiv (x^n-1)^q \mod p$ so that Lemma 4.3.3 still applies to any factor g of f.

As we have noted, this method allows us to deduce non-trivial lower bounds on the Mahler measure even when r is large. There is the disadvantage that q is potentially much larger than r, making the inequalities of Lemma 4.3.3 weaker than those of Lemma 4.3.2 in some cases. Furthermore, if m has many prime factors, p will be significantly smaller than m, again making the inequalities of Lemma 4.3.3 weaker than those of Lemma 4.3.2.

As a general rule, we will use Lemma 4.3.2 when r is small and Lemma 4.3.3 when r is large to obtain the best universal results. We see this strategy in the proof of our next lemma.

Lemma 4.3.4. *Suppose that $f \in \mathbb{Z}[x]$ has degree nr and $f(x) \equiv (x^n - 1)^r \mod m$. If g is a factor of f over $\mathbb{Z}$ having no cyclotomic factors then*

$$\mu(g) \geq \log\left(\frac{m}{2^r}\right)\left(\frac{\deg g}{nr}\right). \tag{4.3.8}$$

If p is a prime dividing m then

$$\mu(g) \geq \frac{1}{p}\log\left(\frac{p}{2}\right)\left(\frac{\deg g}{nr}\right) \tag{4.3.9}$$

and if 2 divides m then

$$\mu(g) \geq \frac{\log 2}{4}\left(\frac{\deg g}{nr}\right). \tag{4.3.10}$$

Proof. To prove (4.3.8), we apply Lemma 4.3.2 with $T(x) = x^n - 1$ and the inequality follows immediately.

To prove (4.3.9), we let p be a prime dividing m and set $q = p^{\lceil \log_p r \rceil}$. Therefore q is an integer greater than or equal to r so that $(x^n-1)^{q-r} f(x) \equiv (x^n-1)^q \mod p$. Using $T(x) = x^n - 1$ with inequality (4.3.6) of Lemma 4.3.3 we find that

$$\mu(g) \geq \log\left(\frac{p}{2}\right)\left(\frac{\deg g}{nq}\right).$$

But we also know that $q = p^{\lceil \log_p r \rceil} < p^{1+\log_p r} = pr$ so that

$$\mu(g) \geq \log\left(\frac{p}{2}\right)\left(\frac{\deg g}{npr}\right)$$

which is the desired inequality.

Finally, to prove (4.3.10), suppose that $2 \mid m$ and $q = 2^{\lceil \log_2 r \rceil}$. Use $T(x) = x^{2n} - 1$ in inequality (4.3.7) of Lemma 4.3.3 to obtain the desired result. □

Proof of Theorem 4.3.1. Let $c_0 = c/(2\log 2)$. We distinguish the following 3 cases.

i. $m \geq 2^{r+c_0}$,

ii. $m < 2^{r+c_0}$ and $2 \mid m$,

iii. $m < 2^{r+c_0}$ and $2 \nmid m$.

If $m \geq 2^{r+c_0}$ then we use inequality (4.3.8) of Lemma 4.3.4 to find that

$$\mu(g) \geq c_0 \log 2 \left(\frac{\deg g}{nr}\right) \geq 2c_0 \log 2 \left(\frac{\deg g}{n2^r}\right) = c \cdot \left(\frac{\deg g}{n2^r}\right).$$

If $m < 2^{r+c_0}$ and $2 \mid m$ then inequality (4.3.10) implies that

$$\mu(g) \geq \frac{\log 2}{4} \left(\frac{\deg g}{nr}\right) \geq \frac{\log 2}{2} \left(\frac{\deg g}{n2^r}\right) \geq c \cdot \left(\frac{\deg g}{n2^r}\right).$$

If $m < 2^{r+c_0}$ and $p \neq 2$ is a prime dividing m then we apply inequality (4.3.9) to find that

$$\begin{aligned}
\mu(g) &\geq \frac{1}{p} \log\left(\frac{p}{2}\right) \left(\frac{\deg g}{nr}\right) \\
&\geq \left(1 - \frac{\log 2}{\log p}\right) \left(\frac{\log p}{p}\right) \left(\frac{\deg g}{nr}\right) \\
&\geq \left(\frac{\log(3/2)}{\log 3}\right) \left(\frac{\log p}{p}\right) \left(\frac{\deg g}{nr}\right).
\end{aligned}$$

However, the function $(\log x)/x$ is decreasing for $x \geq e$. Since $p \leq m < 2^{r+c_0}$, we conclude that

$$\frac{\log p}{p} > \frac{(r + c_0) \log 2}{2^{r+c_0}} > \frac{r \log 2}{2^{r+c_0}},$$

and hence,

$$\mu(g) \geq \left(\frac{\log(3/2) \log 2}{2^{c_0} \log 3}\right) \left(\frac{\deg g}{n2^r}\right).$$

We know that $2^{c_0} = e^{c/2}$ so that by our definition of c we obtain

$$\mu(g) \geq c \cdot \left(\frac{\deg g}{n2^r}\right)$$

which establishes the theorem in the final case. □

4.4 Polynomials near polynomials of low Archimedean supremum norm

Suppose that m is a non-zero algebraic number. Recall that we write $\nu_\infty(T) = \sum_{v|\infty} \nu_v(T)$ and we say that $f \equiv T \mod m$ if $\nu_v(T-f) \leq \log |m|_v$ for all $v \nmid \infty$. We now examine the situation where f and T are polynomials over $\overline{\mathbb{Q}}$ of the same degree with $f \equiv T \mod m$. If K is a number field containing m with v indexing the places of K, let

$$N(m) = \sum_{v|\infty} \log |m|_v = -\sum_{v\nmid\infty} \log |m|_v.$$

Note that this definition does not depend on K and the second equality follows from the product formula.

Theorem 4.4.1. *Suppose that f and T are polynomials over $\overline{\mathbb{Q}}$ of the same degree such that $f \equiv T \mod m$. If α satisfies $f(\alpha) = 0$ and $T(\alpha) \neq 0$ then*

$$\deg T \cdot h(\alpha) \geq N(m) - \nu_\infty(T).$$

Proof. Let K be a number field containing α, m, the coefficients of T and the coefficients of f. By Theorem 4.1.2 we find that

$$-\deg T \cdot h(\alpha) \leq \sum_{v\nmid\infty} U_v(\alpha, T) + \nu_\infty(T).$$

If $v \nmid \infty$ then $U_v(\alpha, T) \leq \nu_v(T - f) \leq \log |m|_v$ and the result follows. □

Clearly, in order for Theorem 4.4.1 to yield a nontrivial lower bound, we must have that $N(m) > \nu_\infty(T)$, justifying the title of this section. That

is, if f is sufficiently close to T at enough non-Archimedean places of K, the positive contribution from $N(m)$ will overcome the negative contribution from $\nu_\infty(T)$. We also note the special case of Theorem 4.4.1 where $m \in \mathbb{Z}$ and $f, T \in \mathbb{Z}[x]$.

Corollary 4.4.2. *Suppose that f and T are polynomials over $\mathbb{Z}$ of the same degree and m is a positive integer such that $f \equiv T \mod m$. If g is a factor of f relatively prime to T then*

$$\deg f \cdot \mu(g) \geq \deg g \cdot (\log m - \nu_\infty(T)).$$

Proof. Apply Theorem 4.4.1 to each root α of g and the corollary follows. □

Corollary 4.4.3. *Suppose that f and T are polynomials over $\mathbb{Z}$ of the same degree and m is a positive integer such that $f \equiv T \mod m$. If f is relatively prime to T then*

$$\mu(f) \geq \log m - \nu_\infty(T).$$

Proof. Apply Corollary 4.4.2 with $g = f$ and the result is immediate. □

Chapter 5

Lower Bounds of the Heights of Algebraic Points [12]

5.1 Main Results

We follow the techniques of Beukers and Zagier [2]. Suppose that $r, n_1, \ldots, n_r$ are positive integers and K is a field. Then we write $\mathcal{P}(K) = \mathbb{P}^{n_1}(K) \times \cdots \times \mathbb{P}^{n_r}(K)$ and denote the coordinates by $\mathbf{x} = (\mathbf{x}_0, \ldots, \mathbf{x}_r)$ with $\mathbf{x}_i = (x_{i0}, \ldots, x_{in_i})$. If $\mathbf{x}$ has $x_{ij} \neq 0$ for all i, j let $\mathbf{x}^{-1}$ be the point obtained by replacing each coordinate x_{ij} of $\mathbf{x}$ with x_{ij}^{-1}. Following [2], choose any subset I of $\{i | n_i = 1\}$ and let $E = \{(i, 0) | i \in I\}$. We refer to E as the set of *exceptional index pairs*. Index pairs not in E are called *regular index pairs*. If a regular index pair appears in a monomial of a polynomial $Q(\mathbf{x})$, then we say the monomial is a *regular monomial* of Q. Otherwise, the monomial is called an *exceptional monomial*. Also write $\|Q\|_v$ to denote the sum of the v-adic absolute values (using $\|\cdot\|_v$) of the coefficients of Q.

Let F be a multihomogeneous polynomial over $\overline{\mathbb{Q}}$ of multidegrees $d_1, \ldots, d_r$ so that F defines a zero set in $\mathcal{P}(\overline{\mathbb{Q}})$. The degree of F in the variable x_{ij} is denoted d_{ij} and define $\tilde{d}_i = -d_i + \sum_j d_{ij}$. Then we set

$$\delta = \max\left\{ \max_{i \in I}\left\{ \frac{\tilde{d}_i + d_{i1}}{n_i + 1} \right\}, \max_{i \notin I}\left\{ \frac{\tilde{d}_i}{n_i + 1} \right\} \right\}$$

and assume that F has the following properties:

(i) the coefficients of F are totally real algebraic integers

(ii) the coefficients of regular monomials of F are integers.

Then for v Archimedean define

$$c(F, v, i, j) = \left\| \frac{\partial F}{\partial x_{ij}} \right\|_v .$$

In [2], Beukers and Zagier consider only polynomials F having integer coefficients, so clearly $c(F, v, i, j)$ does not depend on the place v. In fact, $c(F, v, i, j)$ is defined in [2] using the usual absolute value on the complex numbers rather than $\|\cdot\|_v$. Since we assume only the weaker conditions *(i)* and *(ii)*, $c(F, v, i, j)$ may indeed depend on v as the notation suggests. Therefore, we require the absolute value $\|\cdot\|_v$ in this definition.

However, in the special case that $(i, j) \notin E$, $c(F, v, i, j)$ depends only on the regular monomials of F. So by property *(ii)*, $c(F, v, i, j)$ depends only on the monomials of F having integer coefficients, and therefore, does not depend on v. Then we may define

$$C_F = C_F(E) = \max_{(i,j)\notin E} c(F, v, i, j)$$

and by our remarks above, C_F does not depend on v. We now state our main theorem which is a direct generalization of the main theorem in [2].

Theorem 5.1.1. *Let F be a multihomogeneous polynomial satisfying properties (i) and (ii) above for some exceptional set E. If $\mathbf{x} \in \mathcal{P}(\overline{\mathbb{Q}})$ is such that $F(\mathbf{x}) = 0$, $\prod_{i,j} x_{ij} \neq 0$ and $F(\mathbf{x}^{-1}) \neq 0$ then*

$$\sum_{i=1}^{r} (n_i + 1) H(\mathbf{x}_i) \geq \log \rho$$

where ρ is the unique real root larger than 1 of $x^{-2} + C_F^{-1} x^{-\delta} = 1$.

Once again, we note that our theorem generalizes [2] in that we allow the coefficients of F to come from a potentially larger set. While the main theorem in [2] requires these coefficients to be rational integers, we allow some of them to be totally real algebraic integers.

Before we prove Theorem 5.1.1 we demonstrate its relationship to our problem. Consider r non-zero algebraic numbers $\alpha_1, \ldots, \alpha_r$ such that $\alpha_1 + \cdots + \alpha_r = N$ and $\alpha_1^{-1} + \cdots + \alpha_r^{-1} \neq N$. Corollary 2.1 of [2] gives a lower bound on $\sum_{i=1}^{r} h(\alpha_i)$ when N is an integer. We apply Theorem 5.1.1 to prove a direct generalization of this result.

Corollary 5.1.2. *Suppose $\alpha_1, \ldots, \alpha_r$ are non-zero algebraic numbers and N is a totally real algebraic integer. If $\alpha_1 + \cdots + \alpha_r = N$ and $\alpha_1^{-1} + \cdots + \alpha_r^{-1} \neq N$ then*

$$\sum_{i=1}^{r} h(\alpha_i) \geq \frac{1}{2} \log \frac{1 + \sqrt{5}}{2}$$

with equality when $r = 1$ and $\alpha_1 = \frac{1+\sqrt{5}}{2}$.

Proof. Write $\alpha_i = \alpha_{i1}$ for all i and suppose that the α_{i0} are algebraic numbers. We consider the point

$$\boldsymbol{\alpha} = (\alpha_{10}, \alpha_{11}) \times \cdots \times (\alpha_{r0}, \alpha_{r1}) \in (\mathbb{P}^1(\overline{\mathbb{Q}}))^r.$$

We will apply Theorem 5.1.1 to this point with $I = \{1, \ldots, r\}$ so we have $E = \{(1,0), \ldots, (r,0)\}$. Let F be the homogeneous version of $x_{10}+\cdots+x_{r0}-N$. That is,

$$F(\mathbf{x}) = \sum_{i=1}^{r} x_{i1} \prod_{j \neq i} x_{j0} - N \prod_{j} x_{j0}$$

and note that F satisfies properties *(i)* and *(ii)*. It is clear that $c(F, v, i, j) = 1$ for all $(i, j) \notin E$ so that $C_F = 1$. We also have $n_i = 1$, $d_i = 1$ and $d_{i1} = 1$ so that $\delta = 1$. Then by Theorem 5.1.1

$$\sum_{i=1}^{r} 2H(\alpha_{i0}, \alpha_{i1}) \geq \log \rho$$

where ρ is the real root larger than 1 of $x^{-2} + x^{-1} = 1$. Setting $\alpha_{i0} = 1$ for all i the result follows and the case of equality is clear. □

Note that the case of equality in Corollary 5.1.2 is not unique. For example, we also have equality when $r = 2$, $\alpha_1 = 1$ and $\alpha_2 = \frac{1+\sqrt{5}}{2} - 1$. Several other cases of equality are given in [2] and [16] using integer values for N.

In the special case that $r = 1$ Corollary 5.1.2 implies that $h(\alpha) \geq \frac{1}{2} \log \frac{1+\sqrt{5}}{2}$ for all totally real algebraic integers $\alpha \notin \{0, \pm 1\}$. Therefore, Schinzel's bound [14] on the height of a totally real algebraic integer is a corollary of our result.

Corollary 5.1.3. *If α is a totally real algebraic integer with $\alpha \notin \{\pm 1, 0\}$, then*

$$h(\alpha) \geq \frac{1}{2} \log \frac{1+\sqrt{5}}{2}.$$

5.2 Proof of Theorem 5.1.1

We begin with some additional notation. Recall that for a point $\mathbf{x} \in \mathcal{P}(K)$ for some field K we denote the coordinates $\mathbf{x} = (\mathbf{x}_1, \ldots, \mathbf{x}_r)$ with $\mathbf{x}_i = (x_{i0}, \ldots, x_{in_i})$. Similarly, for a point $\mathbf{m} \in \mathbb{Z}^{n_1+1} \times \cdots \times \mathbb{Z}^{n_r+1}$ we set $\mathbf{m} = (\mathbf{m}_1, \ldots, \mathbf{m}_r)$ with $\mathbf{m}_i = (m_{i0}, \ldots, m_{in_i})$. Define the product $\mathbf{x}^{\mathbf{m}} = \prod_{i,j} x_{ij}^{m_{ij}}$ and the set

$$M = \left\{ \mathbf{m} \in \mathbb{Z}^{n_1+1} \times \cdots \times \mathbb{Z}^{n_r+1} \,\middle|\, m_{ij} \geq 0,\ \sum_j m_{ij} = d_i \ \forall i \right\}$$

so that the polynomial F may be written

$$F(\mathbf{x}) = \sum_{\mathbf{m} \in M} s_{\mathbf{m}} \mathbf{x}^{\mathbf{m}}$$

where the $s_{\mathbf{m}}$ are totally real algebraic integers. Let $\{G_k(x)\}$ be a finite collection of multihomogeneous polynomials over K with algebraic integer coefficients. Assume that G_k has multidegrees $d_{k1}, \ldots, d_{kr}$. As above, we define the sets

$$M_k = \left\{ \mathbf{m} \in \mathbb{Z}^{n_1+1} \times \cdots \times \mathbb{Z}^{n_r+1} \,\middle|\, m_{ij} \geq 0,\ \sum_j m_{ij} = d_{ki} \ \forall i \right\}$$

and write

$$G_k(\mathbf{x}) = \sum_{\mathbf{m} \in M_k} s_{k\mathbf{m}} \mathbf{x}^{\mathbf{m}}$$

where the $s_{k\mathbf{m}}$ are algebraic integers.

If K is a number field containing the coefficients of the polynomials G_k and v is a place of K we write $X(K)$ to denote the zero set of F in $\mathcal{P}(K)$ and $X(K_v)$ for the zero set of F in $\mathcal{P}(K_v)$. Let

$$\Delta_v(K) = \{\mathbf{x} \in \mathcal{P}(K) \mid \|x_{ij}\|_v \leq 1 \ \forall i, j\}$$

and

$$\Delta(K_v) = \{\mathbf{x} \in \mathcal{P}(K_v) \mid \|x_{ij}\|_v \leq 1 \ \forall i, j\}.$$

Then define $X_v(K)_1 = X(K) \cap \Delta_v(K)$ and $X(K_v)_1 = X(K_v) \cap \Delta(K_v)$ and observe that $X_v(K)_1 \subset X(K_v)_1$. Our first Lemma is an analog of Lemma 3.1 of [2].

Lemma 5.2.1. *Suppose that K is any number field containing the coefficients of the polynomials G_k, that v indexes the places of K, and that $a_k \geq 0$ for all k. Set*

$$w_i = \sum_k a_k d_{ki}, \qquad \log \lambda_v = - \max_{\mathbf{x} \in X(K_v)_1} \left\{ \sum_k a_k \log \|G_k(\mathbf{x})\|_v \right\}.$$

If $\mathbf{x} \in X(K)$ with $\prod_k G_k(\mathbf{x}) \neq 0$ then

$$\sum_{i=1}^{r} w_i H(\mathbf{x}_i) \geq \sum_{v|\infty} \frac{D_v}{D} \log \lambda_v.$$

Proof. We will prove that the local inequality

$$\sum_{i=1}^{r} w_i \log(\max_j \|x_{ij}\|_v) \geq \sum_k a_k \log \|G_k(\mathbf{x})\|_v + \begin{cases} \log \lambda_v & \text{if } v \mid \infty \\ 0 & \text{if } v \nmid \infty \end{cases} \tag{5.2.1}$$

holds for all places v of K.

We first assume that $v \nmid \infty$. Since each coefficient $s_{k\mathbf{m}}$ of G_k is an algebraic integer, we have that $\|s_{k\mathbf{m}}\|_v \leq 1$ for all $k, \mathbf{m}$. By the strong triangle inequality, there exists $\mathbf{m} \in M$ such that

$$\begin{aligned}\sum_k a_k \log \|G_k(\mathbf{x})\|_v &\leq \sum_k a_k \log \|\mathbf{x}^{\mathbf{m}}\|_v \\ &= \sum_k a_k \sum_i d_{ki} \log \max_j \|x_{ij}\|_v \\ &= \sum_i w_i \log \max_j \|x_{ij}\|_v\end{aligned}$$

and we have established (5.2.1) in the case that $v \nmid \infty$.

Next we assume that $v|\infty$. For each i, let $j_0 = j_0(i)$ be such that $\max_j \|x_{ij}\|_v = \|x_{ij_0}\|_v$. Let $\mathbf{x}'$ be the point obtained by replacing each coordinate of $\mathbf{x}$ with x_{ij}/x_{ij_0}. We have that $\|x_{ij}/x_{ij_0}\|_v \leq 1$ for all i, j so that

$$\sum_{i=1}^r w_i \log \max_j \left\| \frac{x_{ij}}{x_{ij_0}} \right\|_v \geq \sum_k a_k \log \|G_k(\mathbf{x}')\|_v + \log \lambda_v$$

By the homogeneity of the polynomials G_k we find that

$$\begin{aligned}\sum_k a_k \log \|G_k(\mathbf{x}')\|_v &= \sum_k a_k \log \left\| \prod_i x_{ij_0}^{-d_{ki}} G_k(\mathbf{x}) \right\|_v \\ &= \sum_k a_k \log \|G_k(\mathbf{x})\|_v - \sum_i w_i \log \|x_{ij_0}\|_v\end{aligned}$$

and conclude that

$$\sum_{i=1}^r w_i \log(\max_j \|x_{ij}\|_v) \geq \sum_k a_k \log \|G_k(\mathbf{x})\|_v + \log \lambda_v$$

so we have established (5.2.1). Now sum both sides of (5.2.1) over all places v of K and apply the product formula. The desired result follows. $\square$

Note that in the version of Lemma 5.2.1 that appears in [2], the polynomials G_k are assumed to have integer coefficients. Therefore, each λ_v is in fact independent of v. In this simpler situation, Beukers and Zagier define λ_v using the usual absolute value on $\mathbb{C}$ rather than $\|\cdot\|_v$ on K_v.

In our version of Lemma 5.2.1 we allow for the G_k to have any algebraic integer coefficients, so we must define λ_v using $\|\cdot\|_v$ on a number field containing the coefficients of the G_k. It is certainly possible that λ_v does indeed depend on the place v. However, with appropriate choices for G_k and a_k, conditions (i) and (ii) are enough to produce a universal lower bound on λ_v that does not depend on v. In view of Lemma 5.2.1, this lower bound gives a bound on $\sum_{i=1}^{r}(n_i+1)H(\mathbf{x}_i)$.

Before we make selections for the G_k and the a_k, we state Lemmas 3.2 and 3.3 of [2] for use later. Although the statement of Lemma 3.2 in [2] is for polynomials with integer coefficients, it is easily verified that the lemma holds for polynomials with complex coefficients and we state this generalization here.

Lemma 5.2.2. *Suppose v is a complex Archimedean place of a number field K. If $Q_k(\mathbf{x})$ are multihomogeneous polynomials with coefficients in K_v then the function $\sum_k a_k \log\|Q_k(\mathbf{x})\|_v$ assumes a maximum in $X(K_v)_1$ at a point $\mathbf{x}$. Moreover, $\mathbf{x}$ has one coordinate pair (i_0, j_0) such that $\|x_{ij}\|_v = 1$ for all $(i,j) \neq (i_0, j_0)$.*

Lemma 5.2.3. *let $\alpha, \beta, \gamma > 0$ Let l be the unique minimum of the function*

$$u \log \frac{\gamma u}{u+v} + v \log \frac{v}{u+v}$$

under the constraints $u, v \geq 0$, $\alpha u + \beta v = 1$. *Then* e^{-l} *is the unique real root larger than* 1 *of* $\gamma^{-1}x^{-\alpha} + x^{-\beta} = 1$.

We now make our selections for G_k and a_k following [2]. For G_k we choose the coordinates x_{ij} and the polynomial

$$\tilde{F}(\mathbf{x}) = F(\mathbf{x}^{-1}) \prod_{i,j} x_{ij}^{d_{ij}}.$$

Note that $\tilde{F}$ is multihomogeneous with multidegrees given by $\tilde{d_i} = -d_i + \sum_j d_{ij}$. Write a_{ij} and b for the values of a_k corresponding to x_{ij} and $\tilde{F}$, respectively. In this situation we have

$$\log \lambda_v = - \max_{\mathbf{x} \in X(K_v)_1} \left\{ \sum_{i,j} a_{ij} \log \|x_{ij}\|_v + b \log \|\tilde{F}(\mathbf{x})\|_v \right\}. \tag{5.2.2}$$

Finally, let ρ be the real root greater than 1 of $x^{-2} + C_F^{-1} x^{-\delta} = 1$.

Lemma 5.2.4. *Suppose* K *is a number field containing the coefficients of* F *and* $D_v = 2$ *for all Archimedean places* v *of* K. *Then there exist* $a_{ij}, b \geq 0$ *such that* $n_i + 1 = \sum_j a_{ij} + b\tilde{d_i}$ *for all* i *and* $\lambda_v \geq \rho$ *for all* $v|\infty$.

Proof. Following [2], we define each a_{ij} in terms of b by

$$a_{ij} = 1 - \frac{\tilde{d_i}}{n_i + 1} b \quad \text{if } i \notin I \tag{5.2.3}$$

and

$$a_{ij} = 1 - \frac{\tilde{d_i} + (-1)^j d_{i1}}{n_i + 1} b \quad \text{if } i \in I \tag{5.2.4}$$

so we immdiately have $n_i + 1 = \sum_j a_{ij} + b\tilde{d_i}$. Now we need only select b so that $\lambda_v \geq \rho$.

We will show that under the assumptions (5.2.3) and (5.2.4)

$$-\log \lambda_v \leq b \log \frac{2bC_F}{(1-\delta b)+2b} + \frac{1-\delta b}{2} \log \frac{1-\delta b}{(1-\delta b)+2b} \tag{5.2.5}$$

holds for every Archimedean place v of K. Let

$$\Phi(\mathbf{x}) = \sum_{i,j} a_{ij} \log \|x_{ij}\|_v + b \log \|\tilde{F}(\mathbf{x})\|_v$$

so that we must give an upper bound on $-\log \lambda_v = \max_{\mathbf{x} \in X(K_v)_1} \Phi(\mathbf{x})$. By Lemma 5.2.2 this maximum is attained at a point $\mathbf{x} \in X(K_v)_1$ where $\|x_{i_0 j_0}\|_v \leq 1$ for some coordinate pair (i_0, j_0) and $\|x_{ij}\|_v = 1$ for all $(i,j) \neq (i_0, j_0)$. Hence, $\bar{x}_{ij} = x_{ij}^{-1}$ for all $(i,j) \neq (i_0, j_0)$. Moreover, $\Phi(\mathbf{x}) \to -\infty$ as $x_{ij} \to 0$ for any i, j. Therefore, we must have $x_{i_0 j_0} \neq 0$ so that the point $\mathbf{x}^{-1}$ is well defined.

Suppose first that $(i_0, j_0) \notin E$ and write $x = x_{i_0 j_0}$, $d = d_{i_0 j_0}$ and $m = m_{i_0 j_0}$ for any $\mathbf{m} \in M$. Let $\bar{\mathbf{x}}$ be the point obtained by replacing each coordinate of $\mathbf{x}$ with $\bar{x}_{ij}$. By property (i), the coefficients of F are in the fixed field of complex conjugation in K_v. Using $F(\mathbf{x}) = 0$ we obtain

$$\begin{aligned} F(\mathbf{x}^{-1}) &= F(\mathbf{x}^{-1}) - F(\bar{\mathbf{x}}) \\ &= \sum_{\mathbf{m} \in M} s_{\mathbf{m}} \mathbf{x}^{-\mathbf{m}} - \sum_{\mathbf{m} \in M} s_{\mathbf{m}} \bar{\mathbf{x}}^{\mathbf{m}} \\ &= \sum_{\mathbf{m} \in M} s_{\mathbf{m}} \left(\frac{\bar{\mathbf{x}}^{\mathbf{m}}}{\bar{x}^m} \right) (x^{-m} - \bar{x}^m) \end{aligned}$$

and note that $\|\bar{\mathbf{x}}^{\mathbf{m}} / \bar{x}^m\|_v = 1$ for all $\mathbf{m} \in M$. We now apply the triangle

inequality to find

$$\begin{aligned}\|\tilde{F}(\mathbf{x})\|_v &\le \|x\|_v^d \sum_{\mathbf{m}\in M} \|s_{\mathbf{m}}(x^{-m} - \bar{x}^m)\|_v \\ &\le \|x\|_v^d \cdot \|x^{-1} - \bar{x}\|_v \sum_{\mathbf{m}\in M} m\|s_{\mathbf{m}}\|_v \cdot \|x^{-1}\|_v^{m-1} \\ &\le \|x\|_v^d \cdot \|x^{-1} - \bar{x}\|_v \cdot \|x\|_v^{1-d} \sum_{\mathbf{m}\in M} m\|s_{\mathbf{m}}\|_v \\ &= c(F, v, i_0, j_0)(1 - \|x\|_v^2),\end{aligned}$$

where the last equality follows since $c(F, v, i_0, j_0) = \sum_{\mathbf{m}\in M} m\|s_{\mathbf{m}}\|_v$. Now let $\xi = \|x\|_v^2$, $c = c(F, v, i_0, j_0)$ and $a = a_{i_0 j_0}$. We have

$$-\log \lambda_v \le \max_{\xi\in[0,1]} \left(b \log(c(1-\xi)) + \frac{a}{2} \log \xi \right).$$

Differentiating we find that this maximum is attained at $\xi_0 = a/(a+2b)$ and its value is

$$b \log \frac{2bc}{a+2b} + \frac{a}{2} \log \frac{a}{a+2b}. \tag{5.2.6}$$

By definition $a = 1 - b\tilde{d_i}/(n_i+1) \ge 1 - \delta b$. Therefore (5.2.6) is bounded above by

$$b \log \frac{2bC_F}{(1-\delta b)+2b} + \frac{1-\delta b}{2} \log \frac{1-\delta b}{(1-\delta b)+2b}$$

and (5.2.5) follows.

Next assume that $(i_0, j_0) \in E$ so that $j_0 = 0$. We have that $\|x_{i_0 0}\| \le 1$ and $\|x_{ij}\| = 1$ for all $(i, j) \ne (i_0, 0)$. We write $x = x_{i_0 0}$, $x' = x_{i_0 1}$, $d = d_{i_0 0}$,

$d' = d_{i_0 1}$, $m = m_{i_0 0}$ and $m' = m_{i_0 1}$ for each $\mathbf{m} \in M$. Then we find

$$\begin{aligned}
\|\tilde{F}(\mathbf{x})\|_v &= \|x^d F(\mathbf{x}^{-1}) - \bar{x}^{-d} F(\bar{\mathbf{x}})\|_v \\
&= \left\| \sum_{\mathbf{m} \in M} s_{\mathbf{m}} \left(\frac{\bar{\mathbf{x}}^{\mathbf{m}}}{\bar{x}^m} \right) (x^{d-m} - \bar{x}^{m-d}) \right\|_v \\
&\leq \sum_{\mathbf{m} \in M} \|s_{\mathbf{m}} (x^{d-m} - \bar{x}^{m-d})\|_v \\
&\leq \|x - \bar{x}^{-1}\|_v \cdot \sum_{\mathbf{m} \in M} (d-m) \cdot \|s_{\mathbf{m}}\|_v \cdot \|x^{-1}\|_v^{d-m-1}
\end{aligned}$$

We know that $m + m' = d_{i_0} \geq d$ so $d - m \leq m'$. Therefore, we obtain

$$\begin{aligned}
\|\tilde{F}(\mathbf{x})\|_v &\leq \|x - \bar{x}^{-1}\|_v \sum_{\mathbf{m} \in M} m' \|s_{\mathbf{m}}\|_v \cdot \|x\|_v^{1-m'} \\
&\leq \|x - \bar{x}^{-1}\|_v \cdot \|x\|_v^{1-d'} \sum_{\mathbf{m} \in M} m' \|s_m\|_v \\
&= (1 - \|x\|_v^2) \cdot \|x\|_v^{-d'} c(F, v, i_0, 1)
\end{aligned}$$

Let $\xi = \|x\|_v^2$ and $c = c(F, v, i_0, 1)$ so that

$$\log \lambda_v \leq \max_{\xi \in [0,1]} \left(b \log(c(1-\xi)) - \frac{d_{i_0 1} b}{2} \log \xi + \frac{a_{i_0 0}}{2} \log \xi \right). \tag{5.2.7}$$

With $a = a_{i_0 0} - d'b$ we have that the right hand side of (5.2.7) equals

$$b \log \frac{2bc}{a + 2b} + \frac{a}{2} \log \frac{a}{a + 2b}.$$

It follows from (5.2.4) that $a \geq 1 - \delta b$ and (5.2.5) holds.

Finally, we select b to make the right hand side of (5.2.5), which does not depend on v, as small as possible. Then we make choices for a_{ij} according to (5.2.3) and (5.2.4). We apply Lemma 5.2.3 with $\alpha = \delta, \beta = 2, \gamma = C_F, u = b$ and $v = (1 - \delta b)/2$. By the lemma, the right hand side of (5.2.5) has a unique

minimum l where e^{-l} is the unique real root larger than 1 of $x^{-2} + C_F x^{-\delta} = 1$. Setting $\rho = e^{-l}$ we establish the lemma. $\square$

Proof of Theorem 5.1.1. Suppose $\mathbf{x} \in \mathcal{P}(\overline{\mathbb{Q}})$ and K is a number field containing all coordinates of $\mathbf{x}$ and all coefficients of F and has $D_v = 2$ for all $v|\infty$. Assume a_{ij}, b are the constants from Lemma 5.2.4 and λ_v is defined as in (5.2.2). Since x_{ij} and $\tilde{F}$ are multihomogeneous and $n_i + 1 = \sum_j a_{ij} + b\tilde{d}_i$, Lemma 5.2.1 implies that

$$\sum_{i=1}^{r}(n_i + 1)\log H(\mathbf{x}_i) \geq \sum_{v|\infty} \frac{d_v}{d} \log \lambda_v$$

whenever $x_{ij} \neq 0$ for all i, j and $F(\mathbf{x}^{-1}) \neq 0$. Then by Lemma 5.2.4 we have $\lambda_v \geq \rho$ so that

$$\sum_{i=1}^{r}(n_i + 1)\log H(\mathbf{x}_i) \geq \sum_{v|\infty} \frac{d_v}{d} \log \rho = \log \rho.$$

$\square$

Bibliography

[1] F. Amoroso and R. Dvornicich, *A lower bound for the height in abelian extensions*, J. Number Theory **80** (2000), no. 2, 260–272.

[2] F. Beukers and D. Zagier, *Lower bounds of heights of points on hypersurfaces*, Acta Arith. **79** (1997), no. 2, 103–111.

[3] E. Bombieri and U. Zannier, *A note on heights in certain infinite extensions of* $\mathbb{Q}$, Atti. Accad. Naz. Lincei Cl. Sci. Fis. Mat. Natur. Rend. Lincei (9) Mat. Appl. **12** (2001), 5–14 (2002).

[4] P. Borwein, E. Dobrowolski and M.J. Mossinghoff, *Lehmer's problem for polynomials with odd coefficients*, preprint (2003).

[5] P. Borwein, K.G. Hare and M.J. Mossinghoff, *The Mahler Measure of polynomials with odd coefficients*, Bull. London Math. Soc. **36** (2004), 332–338.

[6] R. Breusch, *On the distribution of the roots of a polynomial with integral coefficients*, Proc. Amer. Math. Soc. **2** (1951), 939–941.

[7] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*, Acta Arith. **34** (1979), no. 4, 391–401.

[8] A. Dubickas and M.J. Mossinghoff, *Auxiliary polynomials for some problems regarding Mahler's measure*, Acta Arith. **119** (2005), no. 1, 65–79.

[9] D.H. Lehmer, *Factorization of certain cyclotomic functions*, Ann. of Math. **34** (1933), 461–479.

[10] M.J. Mossinghoff, C.G. Pinner and J.D. Vaaler, *Perturbing polynomials with all their roots on the unit circle*, Math. Comp. **67** (1998), 1707–1726.

[11] C.J. Petsche, *The height of algebraic units in local fields*, preprint (2003).

[12] C.L. Samuels, *Lower bounds on the projective heights of algebraic points*, Acta Arith. **125** (2006), no. 1, 41–50.

[13] C.L. Samuels, *The Weil height in terms of an auxiliary polynomial*, Acta Arith., to appear

[14] A. Schinzel, *On the product of the conjugates outside the unit circle of an algebraic number*, Acta Arith. **24** (1973), 385–399. Addendum, ibid. **26** (1975), no. 3, 329–331.

[15] C.J. Smyth, *On the product of the conjugates outside the unit circle of an algebraic integer*, Bull. London Math. Soc. **3** (1971), 169–175.

[16] D. Zagier, *Algebraic numbers close to both 0 and 1*, Math. Comp. **61** (1993), 485–491.

[17] S. Zhang, *Positive line bundles on arithmetic surfaces*, Ann. of Math. **136** (1992), 569–587.

Vita

Charles Lloyd Samuels was born in Boston, Massachusetts, on 14 March 1980, the son of Linda Sue Samuels and Martin Allen Samuels. After completing his work at Buckingham, Browne and Nichols High School, he went on to Williams College where he studied mathematics and received his Bachelor of Arts in June 2002. He moved to Austin and entered the Graduate School at the University of Texas at Austin in August 2002.

Permanent address: The University of Texas at Austin
Department of Mathematics
1 University Station C1200
Austin, Texas 78712

This dissertation was typeset with LaTeX[†] by the author.

[†]LaTeX is a document preparation system developed by Leslie Lamport as a special version of Donald Knuth's TeX Program.